

Proposal No. 830929

Call H2020-SU-ICT-03-2018

Project start: 1 February 2019

Project duration: 47 months



Cyber Security for Europe

D9.21

Final conference on the project results

Document Identification	
Due date	31 December 2022
Submission date	
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	TDL	Lead Author	David Goodman (TDL)
Contributing Beneficiaries	-	Related Deliverables	-

Abstract: This deliverable reports on the Momentum! summit event which took place on 1 and 2 December 2022 at the Representation of the State of Hessen to the EU in Brussels and was live streamed online.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.



Executive Summary

This deliverable reports on the Momentum! summit event which took place on 1 and 2 December 2022 at the Representation of the State of Hessen to the EU in Brussels and was live streamed online. The event comprised several distinct but interrelated components:

- presentations by each of the ten work package leaders
- keynote addresses by three distinguished speakers from the perspectives of government, industry and technology
- presentations from the owners of the six key exploitable results chosen through a filtering process carried out by the T9.4 team and the external, independent two-person jury
- an evening panel discussion involving representatives from the European institutions and agencies, as well as a keynote address live streamed from Kyiv.

The event was an opportunity for the project partners to come together for the last time in the context of CyberSec4Europe and, not only reflect on the work carried out over the last four years, but also consider what would come next for the European cybersecurity community that captured the overall theme of the event, 'Forward with Momentum!'

Document information

Contributors

Name	Partner
Ahad Niknia	GUF
Sascha Löbner	GUF
Christine Jamieson	TDL
David Goodman	TDL
Romy Goodman	TDL
Marko Holbl	UM

Reviewers

Name	Partner
Siyanna Lilova	TLEX
Jozef Vyskoc	VAF

History

Version	Date	Authors	Comment
0.01	20 December 2022	David Goodman	1 st draft
1.0	30 December 2022	David Goodman	Final version
1.0	23 January 2023	Ahad Niknia	Final check, preparation and submission

Table of Contents

1	Introduction	1
1.1	Attendance Registration	1
1.2	Agenda	2
1.3	Branding.....	2
1.4	Pre-Event Publicity	3
1.4.1	Website.....	3
1.4.2	Social media	3
1.4.3	ECCC newsletter.....	3
1.4.4	Press release	3
1.5	Application Branding.....	4
1.5.1	Slide templates	4
1.5.2	Conference agendas	5
1.5.3	Conference bags	6
1.6	Stories - The narrative of a European cybersecurity community	6
1.7	Video live streaming and recording	7
2	Welcome	7
3	Work Package Leaders.....	8
3.1	Governance	8
3.2	Blueprint Research & Design	9
3.3	Roadmapping	10
3.4	Application Demonstrators	10
3.5	Education	11
3.6	Tools	11
3.7	Standardisation.....	11
3.8	Dissemination, Communication & Exploitation.....	11
3.9	Community	12
3.10	CyberSec4Europe	13
4	Keynote Speakers.....	14
4.1	Mario Campolargo, Secretary of State for Digitalisation and Administrative Modernisation, Government of Portugal	14
4.2	Oliver Väärtnõu, CEO Cybernetica	15
4.3	Bart Preneel, Head of Computer Security and Industrial Cryptography (COSIC), KU Leuven	19
5	Evening Panel.....	20
5.1	Cybersecurity in Europe: Past, Present and Future.....	21
6	Key Exploitable Results.....	26
6.1	The six presentations.....	26

6.2	The jury summing up	27
6.3	The winners.....	30
7	Application Demonstrator: Supply Chain Security.....	31
8	Seizing The Momentum!.....	31
9	Summary	33
	Annex A: Momentum! Press Release	34
	Annex B: ECCC Newsletter.....	36

List of Figures

Figure 1: The main Momentum! logo.....	2
Figure 2: The website home page promoting Momentum!.....	3
Figure 3: The key exploitable results Powerpoint template.....	4
Figure 4 The keynote speaker Powerpoint template.....	4
Figure 5: The work package leader Powerpoint template.....	4
Figure 6: The Momentum! four page agenda	5
Figure 7: The Momentum! tote bag, mint tin, personal pin badge	6
Figure 8: Stacks of Stories books.....	6
Figure 9: Video streaming on the home page of the website	7
Figure 10: Kai Rannenburg welcoming the audience	8
Figure 11: Natalia presenting governance.....	9
Figure 12: Antonio presenting blueprint research and design	10
Figure 13: Kai presenting CyberSec4Europe's achievements.....	13
Figure 14: Mario giving his keynote presentation from Portugal.....	14
Figure 15: Oliver responding to a question from the audience	16
Figure 16: Bart engaging with the audience	19
Figure 17: The evening panel discussion.....	21
Figure 18: Ievgen giving his keynote speech on the line from Kyiv	21
Figure 19: Ievgen's opening slide.....	22
Figure 20 Tamara explaining a point	23
Figure 21: Stefan asking a question	25
Figure 22: Stelian describing the jurors' approach to innovation.....	29
Figure 23: Stefan announcing one of the winners.....	30
Figure 24: Stelian and Stefan with Vashek Matyas, receiving the trophy on behalf of SecCerts	30
Figure 25: Stelian and Stefan with Giuseppe Manco, with his trophy for EBIDS	30
Figure 26: The EIN Presswire release.....	35
Figure 27: The ECCC news article on Momentum!	36

All photographs used in this report with the exception of figures 1-7, 9, 26 and 27 are © Eric Berghen 2022

List of Tables

Table 1: Geographic distribution of Momentum! registrants	1
---	---

List of Acronyms

<i>A</i>	AAA	Authentication, Authorisation and Accounting
	AI	Artificial Intelligence
	AIOTI	Alliance for the Internet of Things Innovation
<i>B</i>	BEUC	European Consumer Organisation
<i>C</i>	CHECK	Community Hubs of Expertise in Cybersecurity Knowledge
	cPPP	Contractual Public-Private Partnership
	CRA	Cybersecurity Resilience Act
	CVD	Coordinated Vulnerability Disclosure
<i>D</i>	DARPA	Defense Advanced Research Projects Agency
	DG	Directorate General for Communications Networks, Content and Technology
	CONNECT	Technology
	EBIDS	Ensemble Based Intrusion Detection System
<i>E</i>	EC	European Commission
	ECCC	European Cybersecurity Competence Centre
	ECCO	European Cybersecurity Community
	ECSO	European Cyber Security Organisation
	EDPS	European Data Protection Supervisor
	eID	Electronic Identity
	eIDAS	Electronic Identification, Authentication and Trust Services
	EIN	Everyone's Internet News
	ENISA	European Union Agency for Cybersecurity
	EOS	European Organisation for Security
	EU	European Union
	FHE	Fully Homomorphic Encryption
<i>F</i>	FOSAD	Foundations of Security Analysis and Design
<i>G</i>	GDPR	General Data Protection Regulation
<i>I</i>	IdM	Identity Management
	IDSA	Identity Defined Security Alliance
	IEEE	Institute of Electrical and Electronics Engineers
	IETF	Internet Engineering Task Force
	IFIP	International Federation for Information Processing
	IP	Intellectual Property
<i>M</i>	MPC	Multi-Party Computation
<i>N</i>	NCC	National Coordination Centre
	NiS2	Network Information Security 2
	NIST	National Institute of Standards and Technology
	OT	Operational Technology
<i>P</i>	PET	Privacy Enhancing Technology
<i>R</i>	ROCA	Return of Coppersmith's Attack
<i>S</i>	SDO	Standards Development Organisation
	SME	Small- to Medium-sized Enterprises
	SOC	Security Operations Centre
<i>U</i>	UN	United Nations

1 Introduction

The CyberSec4Europe project funding is coming to an end in December 2022 after almost four years. During this time its 43 consortium partners, friends and associates collaborated creatively and effectively across many different domains associated with cybersecurity.

In order to celebrate what we'd done and what is still yet to come, CyberSec4Europe hosted a two-day event, Momentum!, on 1 and 2 December at the Representation of the State of Hessen in central Brussels.

The overall goal of the event was not only to look at our achievements with work leaders reflecting on topics ranging from governance to standardisation, from blueprint research to skills training but also to highlight our visions for the future.

One of the highlights of the event was a showcase of six shortlisted 'key exploitable and innovative assets' for project partners to present or demonstrate. A two-person jury then appointed two winners from the presented assets. Attendees also heard our keynote speakers share their visions and expectations for the coming years from the perspectives of technology, industry and politics. All in all, this was a memorable and unmissable opportunity to learn what we have learnt and what we see as the way forward for the European cybersecurity community.

1.1 Attendance Registration

As with most previous CyberSec4Europe events, the event registration process was managed through the Hessen Representation, available in English, French and German. The total number of registrants as at 30 November was 182.

Their in-person attendance was split as follows:

- Thursday, 1 December - daytime: 126
- Thursday, 1 December - evening: 134
- Friday, 2 December: 114

The number of those registering for online only across the whole of the two days was 29. However, this does not reflect those who attended one or more sessions in person and others online.

The geographic distribution was according to Table 1

EU and EEA				Rest of the World			
Austria	5	France	3	Poland	2	Brazil	1
Belgium	39	Germany	32	Portugal	3	Ghana	8
Croatia	1	Greece	18	Romania	2	India	3
Cyprus	2	Italy	20	Slovenia	3	Saudi Arabia	1
Czech Republic	6	Lithuania	2	Spain	4	Ukraine	2
Denmark	2	Luxembourg	1	Sweden	2	United Kingdom	1
Estonia	5	Netherlands	2			United States	1
Finland	4	Norway	5	Switzerland	2		

Table 1: Geographic distribution of Momentum! registrants

The registrants represented the following types of organisations:

- | | |
|-----------------------|----|
| • Government | 38 |
| • Industry | 19 |
| • Knowledge Institute | 65 |
| • Other | 49 |
| • SME | 11 |

It should be emphasised that not all registrants actually participated in the event as they had indicated; and that some actual attendees did not indeed register.

1.2 Agenda

The agenda across the two days was designed with the following criteria in mind:

- we should provide the opportunity for the work package leaders to reflect on and highlight the work done in their domain but also give an indication of how their work would be followed through in the future;
- interspersed amongst the work package reports, six carefully chosen exploitable assets and solutions that had been distilled from the output of all the project beneficiaries were showcased on the first day, with a two-person jury assessing each one to present their conclusions;
- it was considered important that the summit of CyberSec4Europe's achievements should not be entirely inward looking or even self-congratulatory and for that reason we invited several keynote speakers to present their views on the future of cybersecurity in Europe from different perspectives - government, industry and technology;
- one of the characteristic features of so many project meetings has been the evening panel discussion with expert speakers from the European institutions and agencies. For Momentum! we wanted to invite back some of the speakers who have supported us in the past, but also to introduce a couple of new dimensions so as to show momentum in looking forward.

1.3 Branding

The approach taken to the branding of Momentum! was to put a strong focus on the future, rather than simply present the conference as a review of all the work that had been completed during the lifecycle of the project. The conference wanted to convey a sense of how much more work could be undertaken to build on the achievements of the project partners, and to highlight which project recommendations would have a future impact for policy makers across Europe. In presenting the trajectory of the project, the word 'momentum' seemed to best encapsulate this ambition.

The logo and associated branding for the conference are built on the existing CyberSec4Europe logo and palette used by the project for all its mainstream activities. In addition, the logo gives a sense of energy and action, capturing the spirit of momentum, primarily pushing forward but also looking back reflectively. This branding was followed through in a number of important project applications.



Figure 1: The main Momentum! logo

1.4 Pre-Event Publicity

1.4.1 Website

For the month prior to the event, the banner headline on the CyberSec4Europe home page pointed to the dedicated Momentum! page which contained the latest agenda, with links to the short bios and photos of everyone involved in the event - the keynote speakers, the evening panellists, the CyberSec4Europe partners, the exploitation and innovation jurors and the session moderators.



Figure 2: The website home page promoting Momentum!

1.4.2 Social media

We created Momentum! GIFs for use in posting on Twitter and LinkedIn. These GIFs were also used to provide an animated main screen backdrop during breaks in the conference itself.

1.4.3 ECCC newsletter

Momentum! was announced in the monthly ECCC newsletter on 16 November - see Annex B

1.4.4 Press release

In addition to posting on LinkedIn, a Momentum! press release was issued on the EIN Presswire on the morning of 1 December - see Annex A

1.5 Application Branding

1.5.1 Slide templates



Figure 3: The key exploitable results Powerpoint template

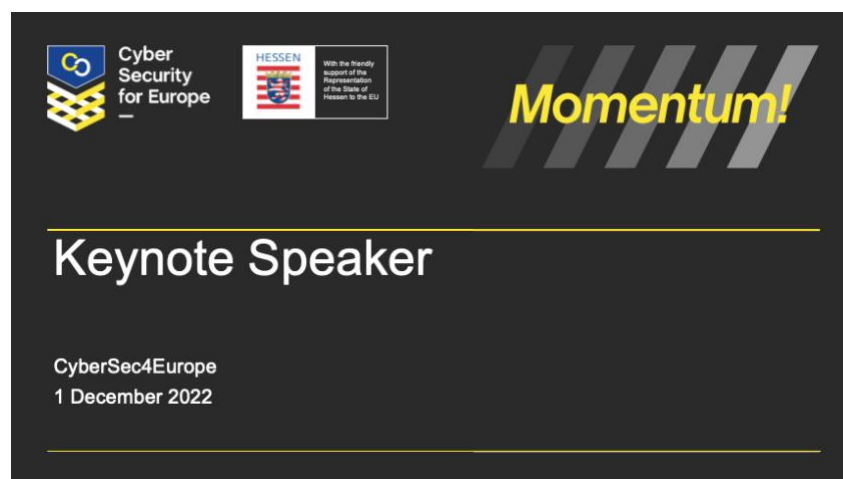


Figure 4 The keynote speaker Powerpoint template



Figure 5: The work package leader Powerpoint template

1.5.2 Conference agendas

Agenda

Momentum!

Thursday 1 December 2022 – Day

11:00 Welcome	Martin Friedrich Reinhardt, Head of Unit, Affairs of the Hessian Ministry of the Interior and for Sports, Representation of the State of Hessen to the EU Kai Rannenberg, Goethe University Frankfurt and CyberSec4Europe coordinator
11:10 Governance	Natalia Koderko, TU Delft
11:35 Achievement	CECIRADA/Therionical Lina Karmi, Cybernetica AS
11:50 Blueprint research & design	Antonio Skarmata, University of Murcia
12:15 Achievement	Kognity Jari Pajunen, IAMK
12:30 Politics keynote	Mário Campelongo, Secretary of State for Digitalisation and Administrative Modernisation, Government of Portugal
13:00	Buffer lunch
	Moderator: Antonio Varmela, CIBIS
14:00 Industry keynote	Olivier Valtinko, C3 O, Cybernetica
14:30 Roadmapping	Evangelos Markatos, FORTH
14:55 Achievement	CyberSec Alessandro Storz, NEC Laboratories Europe GmbH
15:10 Education	Silvia Vidar, University of Trento
15:35 Achievement	Cofe Vincenzo Savarone, Engineering Ingegneria Informatica SpA
15:50	Coffee
16:10 Application demonstrations	Alessandro Storz, NEC Laboratories Europe GmbH
16:35 Achievement	CRIDE Giuseppe Marone, Consiglio Nazionale delle Ricerche (CNR)
16:50 Tools	Vsevolod Matys, Masaryk University
17:15 Achievement	SecCerts, Jyoti Saundh, Masaryk University
17:30 Technology keynote	Dan Prentice, Head of Computer Society and Industrial Cryptography (COSMIC), KMI covers

Agenda

Momentum!

Thursday 1 December 2022 – Evening

18:00	Drinks & snacks
19:00 Welcome	Martin Friedrich Reinhardt, Head of Unit, Affairs of the Hessian Ministry of the Interior and for Sports, Representation of the State of Hessen to the EU Kai Rannenberg, Goethe University Frankfurt and CyberSec4Europe coordinator
19:10 Keynote	Cybersecurity in Europe: Past, Present and Future Igor Vladimirov, International Cybersecurity University, Kyiv
19:20 Discussion panel with special guest speakers	Tamara Tatra, Minister Counsellor, Cyber issues, hybrid threats and disinformation, Permanent Representation of Croatia to the European Union Wojciech Wasieleski, European Data Protection Supervisor (EDPS) Katarzyna Prusak-Górecka, Head of Digital Affairs Unit in Permanent Representation of Poland to the EU, Deputy Chair of the European Cybersecurity Competence Centre Governing Board Francesca Barbara, Programme Officer, Cybersecurity Technology and Capacity Building, DG COMSEC, European Commission Cláudio Teixeira, Legal Officer – Digital and Consumer Rights, The European Consumer Organisation (EUCO)
	Moderator: Kai Rannenberg, Goethe University Frankfurt and CyberSec4Europe coordinator
20:30	Reception

Agenda

Momentum!

Friday 2 December 2022 – Day

08:30	Breakfast
09:00 Achievements review	Italoan Brice, President, C3 O Cluster Sandra Burrell, Founder and CEO, C3PENS & Security GmbH
09:30 Application demonstration	Kognity Matti Wronski, Siemens AG
10:00 Standardisation	Lina Karmi, Cybernetica AS
10:25	Coffee
	Moderator: Christina Jameson, Trust in Digital Life Association
10:50 Communication	David Goodman, Trust in Digital Life Association
11:20 Community	Mark Miller, COMCERTITY
11:45 CyberSec4Europe	Kai Rannenberg, Goethe University Frankfurt and CyberSec4Europe coordinator
12:15	Lunch
13:15 Share the Momentum!	Natalia Koderko, Antonio Skarmata, Evangelos Markatos, Alessandro Storz, Silvia Vidar, Vsevolod Matys, Lina Karmi, David Goodman, Mark Miller Moderator: Kai Rannenberg, CyberSec4Europe coordinator
14:00	Close

Achievements

CyberSec4Europe
Key Exploitable Results

Momentum!



CyberSec4Europe's legacy beyond the end of the project can be seen in the results of the work carried out by all partners over the past four years.

In a series of reports, we highlighted the individual pilot exploitation and innovation plans, involving assets and solutions across the different project domains, ranging from, for example, maritime transport to the 14 digital cyber maps challenges.

As CyberSec4Europe comprises various organisations – from software makers, commercial businesses, universities, research institutes, SMEs, legal and consultancy firms to not-for-profit organisations – each type of partner has evolved exploitation strategies in line with their own needs and opportunities. And we celebrate each and every next.

At Momentum! we are showcasing six of the key exploitable assets and solutions over the course of the first day. As it built up it was to receive the results in six, our independent jury members – led by Chair and other Chair of COSMAS II-Security Unit – will identify not just the top forward to the European Commission Horizon Results Platform.

Demonstrating our achievements

11:35	THEOPH / SPANISH Improving the fight against banking fraud ensuring GDPR compliance and banking security Lina Karmi, Cybernetica AS
12:15	Kognity A mobile cyber security services using a feature rich live cyber maps Jari Pajunen, IAMK
14:55	TEED 102 Digital trust execution environment (TEED) / Subversion needed TEED Alessandro Storz, NEC Laboratories Europe GmbH
15:35	Cofe A context-based personal data suite to manage personal data in compliance with the GDPR Vincenzo Savarone, Engineering Ingegneria Informatica SpA
16:35	CRIDE An ensemble-based intrusion detection system Giuseppe Marone, Consiglio Nazionale delle Ricerche (CNR)
17:15	SecCerts An analysis tool for verification of security products Petr Svenda, Masaryk University
18:00	Close

Figure 6: The Momentum! four page agenda

1.5.3 Conference bags

Every delegate or participant at the event received a tote bag containing the conference agenda, several policy briefs (see D9.28 Policy Recommendations 3), a conference pin, tins of conference-branded mints and a copy of the Stories book.

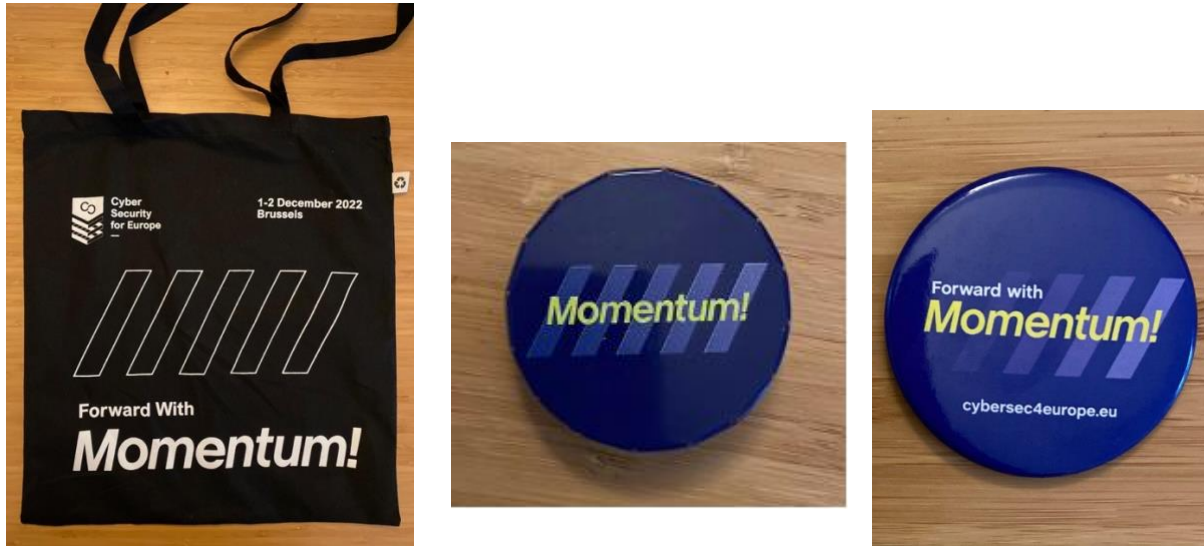


Figure 7: The Momentum! tote bag, mint tin, personal pin badge

1.6 Stories - The narrative of a European cybersecurity community

Stories is the narrative of all the project's achievements, a book to present the life cycle of the project, its achievement and outcomes and the areas that merit future work. This was a summary of all the blog posts, edited by theme, that had been published on the website over the last four years, including deliverable reports mixed with news and opinion pieces. This is a high-quality production to reflect the depth and breadth of the research activities of CyberSec4Europe.



Figure 8: Stacks of Stories books

1.7 Video live streaming and recording

The whole of the two-day event was live-streamed and made available on YouTube and the Home Page of the project website. It also involved remote participation by Mário Campolargo in Portugal, Ievgen Vladimirov in Ukraine and David Goodman in Scotland. The video recordings for both days are available through the CyberSec4Europe YouTube channel and the project website¹.

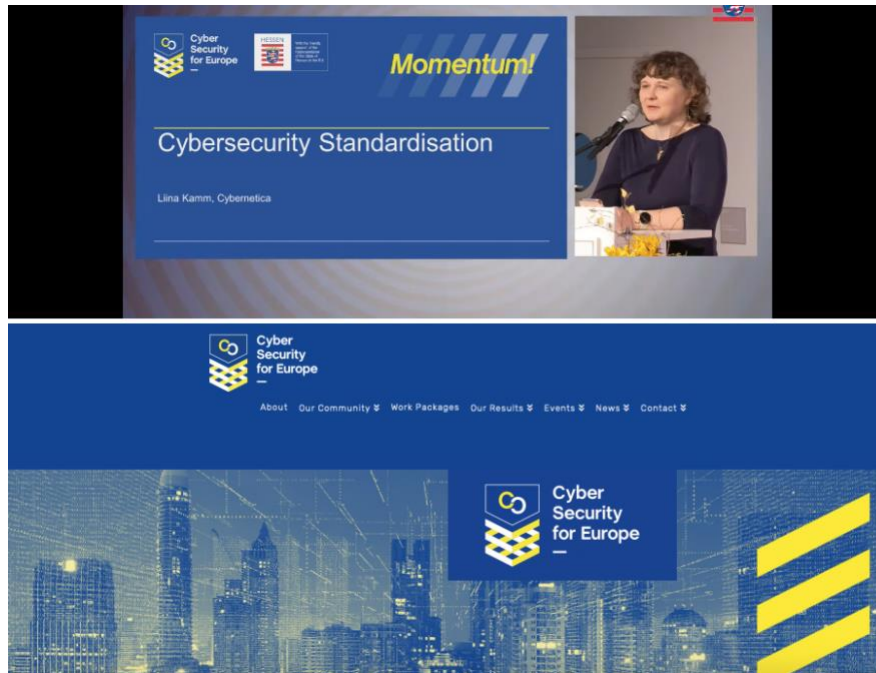


Figure 9: Video streaming on the home page of the website

2 Welcome

Martin Friedrich Reinhardt, Head of Unit, Affairs of the Hessian Ministry of the Interior and for Sports, Representation of the State of Hessen to the EU welcomed the Momentum! conference to the Hessen Representation in Brussels. He told the audience that he was proud of the strong partnership that had grown throughout the years between the Hessen Representation and CyberSec4Europe. He introduced the day's event aimed at looking towards the future with momentum, confident that the conference would be unforgettable.

Kai Rannenberg, Goethe University Frankfurt and CyberSec4Europe coordinator, thanked Herr Reinhardt, the Hessen Representation and its employees for making this event work. He expressed pride about the results CyberSec4Europe had produced over the previous four years. He also looked out into the future and elaborated on how CyberSec4Europe will impact new challenges. Finally, Kai presented the agenda that consisted of a mixture of topical content as well as achievements and exploitable results.

¹ Day one: <https://www.youtube.com/watch?v=8Fo7Pfx2lNA>;
Day two: <https://www.youtube.com/watch?v=XfvKR09QaXA>



Figure 10: Kai Rannenberg welcoming the audience

3 Work Package Leaders

The event comprised short overview presentations from all ten work package leaders, each followed by questions from the audience. All the presentations can be viewed on the CyberSec4Europe website².

3.1 Governance

Natalia I. Kadenko, TU Delft

We developed recommendations for a governance model for the interaction between the ECCC, the NCCs and local cybersecurity communities. We created the concept of CHECKs (Community Hubs of Expertise in Cybersecurity Knowledge) to organise the Community, to address existing challenges, while providing flexibility, accounting for the needs of the local community and creating real added value

We recommended that dedicated funds should be provided, for example, under the Horizon/Digital Europe Programmes, to deepen the cooperation and coordination of such stakeholders, alongside dedicated funds to set up CHECKs in all Member States.

² <https://cybersec4europe.eu/events/momentum/momentum-report/momentum-work-package-leaders/>



Figure 11: Natalia presenting governance

3.2 Blueprint Research & Design

Antonio Skarmeta, University of Murcia

CyberSec4Europe research and innovation was focussed on:

- Privacy-preserving IdM, strong AAA and secure and private communications
- Usability aspects of security assets
- Certification frameworks and continuous monitoring
- Automated tools for verification and enforcement of security policies in software
- GDPR compliance for use in SMEs
- Methodology for the individualised evaluation of requirements
- Advanced threat intelligence services for deploying adaptive security solutions

A functional cybersecurity architecture was developed based on research work, considering 75 software assets, 18 of which were integrated with application demonstrator use cases. In addition, we recorded more than 36 papers in workshops, conferences and journals.



Figure 12: Antonio presenting blueprint research and design

3.3 Roadmapping

Evangelos Markatos, FORTH

We produced three extensive annual reports with an analysis of trends and challenges, as well as short-, medium and long-term roadmaps, in the project's seven application domains:

- Fighting fraud (in Open Banking),
- Supply chain security (and the use of blockchain)
- Privacy-preserving identity management (in Higher Education)
- Incident reporting (in the financial sector)
- Maritime transport
- Medical data exchange
- Smart cities (and the use of personal data)

We participated in the Roadmapping Focus Group with the other pilots, ECSO and in collaboration with the cybersecurity ATLAS to produce a set of priorities in cybersecurity.

3.4 Application Demonstrators

Alessandro Sforzin, NEC Laboratories Europe GmbH

Featuring the seven application domains (see 3.3 Roadmapping), we ran two phases over the course of the project reporting the following:

- A requirements analysis of demonstration use cases
- The specification and set-up of the demonstration use cases
- The validation of the demonstration use cases

The use cases integrated, where appropriate, software assets developed in the project (see 3.2 Blueprint Research). Some of these application areas will be commercially exploited after the end of the project. Altogether 29 use cases were defined identifying the common research, development, and innovation concepts developed by the project and were integrated in 14 demonstrators over the course of the project.

3.5 Education

Jarno Salonen, VTT on behalf of **Silvia Vidor**, University of Trento

The main objective was “to define guidelines and tools that support the design of capability building instruments”. The key questions addressed were:

- Which cybersecurity knowledge areas/units/skills can be taught?
- In which areas/units/skills are we educating people?
- How to choose knowledge areas/units/skills for a specific profile?
- How should an education unit be designed and offered?
- How does one assess and evaluate the quality of an education offer?

A survey was performed to verify which skills are considered important in cybersecurity for academia and industry. The conclusions were that there are critical skills that are not currently being taught by cybersecurity programs; and, at the same time, there are critical mismatches between industrial and academic skills – with seven out of the top ten skills different between the two fields. We produced a collaborative crowd-sourced database of cybersecurity-related education programmes with other pilots and ENISA

3.6 Tools

Vaclav (Vashek) Matyas, Masaryk University

We examined and provided open tools for certification and validation, in close relation to education and standardisation. This included a completely open cyber range – portable, lightweight virtual lab environment.

We worked with and mapped existing cyber ranges and industry requirements and provided specifications for implementation, including a sample integration/federation. We examined the role of certification for cybersecurity and its implementations. We created an ‘Open Tools Portal’ with tools for end-users as well as a set of developed open-source tools for professional use

3.7 Standardisation

Liina Kamm, Cybernetica AS

There were three main objectives: communicate and liaise with SDOs, map standards to application areas and give a comprehensive overview of different SDOs.

We made the following recommendations:

- ECCC should liaise and work with SDOs.
- Standards should be made freely available to universities or independent cybersecurity researchers.
- EC should support standards development and encourage free access to results.
- ECCC could make regular recommendations as to which standards to pick for financing by the EU.
- Member States could support national SDOs to include more international standards in national standardisation collections.
- Member States could translate standards into national languages to increase uptake

3.8 Dissemination, Communication & Exploitation

David Goodman, Trust in Digital Life Association

We managed the project website and social media, weekly news posts/blogs and branding for events, and other purposes. We collected project partner dissemination/communication activities and scientific articles. We also organised events and webinars as well as reported on summer schools involving or organised by partners.

In addition we produced:

- An analysis of SME awareness programmes and recommendations for better outreach based on survey in seven Member States – as well as awareness effectiveness
- Supply chain security recommendations, particularly for SMEs, also based on a narrative of supply chain work across the project
- An exploitation and innovation strategy based on input from all partners
- A series of policy recommendations based on project findings

We provided a report on the dissemination, communication and exploitation activities reflected in the 28 deliverables (mostly reports) which included maintaining the website and regular social media,

- The website grew from small beginnings to contain overview information about the European cybersecurity community from the ECCC and NCCs to the project beneficiaries, associates and friends
- The project's presence on social media has consistently and steadily grown on Twitter, LinkedIn and YouTube
- The Insights series of webinars which were mostly directed by the standardisation team
- Extensive brand development from badges for beneficiaries, associates and friends to distinctive branding for all three concertation events but specifically the two Convergence events; and for Momentum!
- We reported on CyberSec4Europe organisation and participation in summer schools, notably the IFIP and FOSAD
- Under raising awareness, we featured three sub-topics:
 - SME cybersecurity awareness with a particular interest in reaching out to micro-enterprises and non-IT SMEs through national SME federations, and collaboration with the other H2020 projects
 - Supply chain security recommendations created from a narrative built from the work on supply chains from across the project in T4.5, T5.2, WP6 and T9.4
 - Awareness effectiveness, primarily that of cybersecurity programmes
- A regular review of the project beneficiaries strategies for exploitation and innovation including a methodology for filtering the final results leading to the challenge presented at Momentum!
- Policy recommendations

Beyond Momentum!, the social media accounts and the website will continue to be maintained for five years after the end of the project.

Antonio thanked David and the team for doing a great job! Afonso showed his appreciation for the Stories book.

3.9 Community

Mark Miller, CONCEPTIVITY

The objectives were:

- Concertation and clustering with related and concurrent projects for joint learning, information sharing, cooperation, benchmarking and achieving significant impact
- Cooperation with existing cybersecurity ecosystems and communities building upon important experience and capabilities developed over time
- Collaboration with EU bodies and agencies to address the strategic research and innovation agenda elements (cPPP) and to contribute effectively to the work of ENISA, Europol, EU agencies and bodies in relation to cybersecurity

He highlighted the role of CyberSec4Europe regarding community creation and collaboration alongside the activities of the other pilots.

We organised three annual concertation events two of which were branded as CONVERGENCE with recommendations. We reported on partner collaboration with ENISA, DG CONNECT, Europol, ECSO and working groups, EOS, EDPS, IDSA, IETF, IEEE, AIOTI, IoT Forum as well as standardisation bodies. We are looking forward to the results of the ECCO community proposal which will involve stakeholders across many communities.

3.10 CyberSec4Europe

Kai Rannenberg, Goethe University Frankfurt

Following all the individual work package leaders was always going to be difficult, so in consideration Kai provided his reflections on some of the aspects of the CyberSec4Europe journey since February 2019. He reiterated the original aims of the project and how in so many ways we had surpassed expectations, particularly when you look at the pillars and the work packages as a whole.

Kai went on to give an overview of the numerous general meetings, events, keynotes, workshops, and reminded us of the works of art created at the end of many an online internal meeting that started during the pandemic and then took on a life of its own as an expression of the community created amongst partners.

All in all the status CyberSec4Europe achieved was that of a vibrant pilot.

Kai summed up by considering the challenges for the future beyond the end of CyberSec4Europe funding in terms of geopolitics, platforms and European investment in cybersecurity research and development which will be driven by the new infrastructure that the project was funded to pilot.



Figure 13: Kai presenting CyberSec4Europe's achievements

4 Keynote Speakers

There were three keynote speakers representing different external perspectives on cybersecurity

- **Mario Campolargo**, Secretary of State for Digitalisation and Administrative Modernisation, Government of Portugal who previously worked at DG CONNECT
- **Oliver Väärtnõu**, CEO of Cybernetica AS, an Estonian SME
- **Bart Preneel**, Head of Computer Security and Industrial Cryptography (COSIC), at KU Leuven.

4.1 Mario Campolargo, Secretary of State for Digitalisation and Administrative Modernisation, Government of Portugal



Figure 14: Mario giving his keynote presentation from Portugal

Mario is working towards modernisation in the Portuguese government in the sense of digitalisation which requires a new mindset and doing things in a new way, with people being at the centre of this. New technologies have value for companies to develop intelligent territories. We need to tackle cybersecurity as one of the key points. We also need safe digital services. We would like to have better services and not leave anybody behind - a human-centric and whole-society approach. The Portugal presidency has stressed a fair and digital recovery for Europe.

The issues of trust prevent further adoption. Digital technologies are key for a new society and economy but we must ensure safe and trustworthy digital technologies with cybersecurity being one of the components that enables trust. Covid accelerated the migration to cyberspace. It diversified the threats landscape – the current main threats are ransomware and social engineering. Cybersecurity has become a business venture – ransomware as a service or even open-source. Cyber threats accounted for 5.5 trillion EUR. The new political reality is another key aspect that impacts cybersecurity.

The new cybersecurity strategy is important – a safer single digital market. The new Cybersecurity Resilience Act (CRA) shows the direction of development – a critical regulatory instrument to ensure the security of the whole supply chain.

Europe has developed a regulatory framework, but we need to go further. We need to have cybersecurity present in everyday life. Cybersecurity should be seen as an investment, not a cost. CyberSec4Europe is related to these concerns and related to ECCC and the NCCs. The mission of the ECCC is to provide a dedicated approach with the use of the Digital Europe and Horizon Europe programmes in order to facilitate strategic cybersecurity projects and to achieve quorum among Member States, deepen strategies and assure coordination inside the EU.

In summary, Mario believes it is important to foster digital skills and people, by endorsing smart solutions in the private and public sectors and bringing digital (automated) (public) services closer to the citizens. Digitalisation efforts are important for personal (users) and societal perspectives. The issue of threat is present in all aspects of digitalisation: digitalised solutions should be both safe and trustworthy. Mario agrees with the most important issues that ENISA has pointed out in their report, estimating that 10TB of data are stolen every month. The implementation of cybersecurity has to be met with the same ambition and commitment as it is to developing promising new technologies, such as 5G, IoT and AI. The new Cybersecurity Resilience Act and NIS2 directive are good examples of this.

The challenge is to make cybersecurity a part of the everyday lives of people and organisations - how to make it important and relevant to them. The ECCC will help with joint/focused funding/research and European independence and of course national governments play a key role (by how they implement the regulations). Cybersecurity is important for resilience and recovery.

In Portugal, they have C-academy for ICT professionals (public and private) with 44 courses spread across the country. The C-academy is an addition to the more generic training that existed before. Scale and distance from the main centre diminish involvement/intensity. In Portugal, they have, for this reason, a C-network – seven centres spread across Portugal’s regions to give local support in the cybersecurity efforts which are somehow connected to the C-academy and could serve to support the Portuguese NCC. A Cybersecurity Hub was established in Portugal which has produced best practices and some certification possibilities - a national certification scheme following EC certification schemes).

As a result of these initiatives, Portugal recently advanced on the global cybersecurity index from 47th to 14th place.

Question from Kai: How does the implementation so far integrate/translate to the current NCC/ECCC efforts? What do you expect from NCC/ECCC?

Mario: National strategy work has to be aligned with the goals of the EU. National strategies /work /efforts should form /mould /lead the EU goals and policies. Collaboration in the cybersecurity field and with related fields/disciplines is important and connects the goals of Portugal’s efforts and ECCC’s goals.

4.2 Oliver Väärtnõu, CEO Cybernetica

Oliver expressed his thanks for being given the opportunity to provide insights from an industry perspective on cybersecurity.

He started by telling the story of eEstonia with Cybernetica’s place in it, how over the last 60 years an organisation has blended research and development with cybersecurity always at its core.

Cybernetica was founded in 1960 as a research institute called Institute of Cybernetics under the Estonian Academy of Sciences. It was a direct response to Norbert Wiener’s famous book from 1948, which established the discipline of cybernetics, called, as he put it, “Control and Communication in the Animal and the Machine”. The discipline essentially studied how with the use of technology one could make societies and systems more efficient. The Cybernetics Institute was really focused on applied science(s), on how to develop practical solutions, for example, to the mining industry, on how to improve factory production systems etc. At its height, the institute had around 700 employees and was servicing not only Soviet Estonia but also the wider Soviet ecosystem.

Estonia gained its independence at the end of the eighties. All links to Russia were cut and the institute's funding and client base collapsed. That did not only happen to the Institute of Cybernetics, but to all other 15 institutes that existed at that time, plus universities. The Estonian government faced a serious challenge on how to gear its research and innovation system towards its own national goals – what were the goals, what was the optimal innovation system for its current and future needs? A decision was taken that these institutes were to be merged with universities which meant becoming the main research and development agencies in Estonia, of course with radical decrease in funding and personnel.



Figure 15: Oliver responding to a question from the audience

There were a few exceptions, however, the Institute of Cybernetics being one of them. It became a company, which played a key role in creating the new governance structure for Estonia. It had struck a relevant balance between understanding computer science, governance or governance systems and information security (or cybersecurity as the discipline is known today). The first two disciplines are evident from the definition, but information security perhaps not. The decision to start developing information security as a discipline, was taken in the mid-1990s after having seen that IT systems would become prevalent in their usage. The security aspect is one of the most fundamental characteristics in order to guarantee their widespread.

So when Estonia really started to build up its institutions in the mid-1990s (the first years of independence were a transition period), it had the guts and the entrepreneurialism to think what is the new form of government. Perhaps it was not about building brick houses to serve its citizens, but rather something new. Estonia took a plunge, as the Economist magazine noted some years ago.

The politicians who were in their twenties and thirties had heard of computers and a thing called the Internet, perhaps even seen them and played the first computer games, programmed a line of two of code. They created the Tiger Leap Program and organization called the Innovation Fund to engage the researchers to look into the future, to design something new. A digital government, or a digital society? Some of the issues that needed to be solved had to be designed on the societal level rather than only for the governmental purposes.

And so the journey started; funnily enough, it didn't start by creating technology, applications and architectures, it started by creating a relevant legal framework, the rules and regulations for the government to interact in cyberspace, and to do this securely. Creating the norms for technologies that could be used for interacting. Cybernetica had a modest role here in advising the Estonian Parliament on the creation of the Digital Signatures Act and in amending the Public Information Act.

Then came the work on two essential building blocks – on the architecture of the eGovernment system and on identity in cyberspace. Firstly, how does an eGovernment architecture look like for a small country – is it centralised or is it decentralised, what kind of security requirements does it stipulate, what standards does it use? One could argue just like today, in the case of cloud discussions, in order to achieve efficiency, one should put all data into one big repository and use this as a hub for the provision of governmental services. There was a strong school of thought propagating this so-called efficiency-based solution. The other school

of thought, which was put forward by Cybernetica's researchers and engineers, noted that for a democratic society a decentralised system, where organisations interact with each other via peer-to-peer communication, the data resides with the organisations that are responsible for it, and where the security aspects (like certification management, timestamping of the transactions etc) of the system is given to a relevant responsible government body. This system today is called the X-Road, which is basically the operating system of the Estonian eGovernment. It has over 700 organisations connected to it, with annually over 2.7 billion transactions being made from healthcare to transportation. The decisions based on security assessments made in the mid-2000s have enabled this technology to have had zero downtime over the years and enabled it to succumb to the first ever major cyber attacks directed against a nation in 2007. Yes, certain nodes failed, but the system was redundant and stayed operational. Cybernetica is happy to note that based on the experiences learnt from building the Estonian X-Road, it has created a product called the Unified eXchange Platform, which enables to power around ten eGovernment systems around the world, and will be adopted as a base technology for the first ever Japanese Data Bank.

The second building block is identity. In order to provide anybody services on the Internet, one needs to know with whom they are interacting; that is, a strong identity is needed, both from an enrolment perspective, but also from the technology tool perspective as well. Furthermore, imagine the efficiencies for the society (and Oliver fully understands that this is not the case always for all countries) if this identity is universal: that is, it is not only used by governments but also by private and other sectors as well. After extensive technology and security studies, a PKI-based identity card system was opted for. First, a pilot was run, and the cards were enrolled in 2002. It took some years, for people to get accustomed to the card, the private sector to push it, but today there is really no imaginable alternative. Estonians authenticate to all web-based systems (not only government) and sign all documents with their eID tools. Over the years, they have made the infrastructure more resilient, introducing the mobileID and then also Smart-ID, a purely software based eID solution that provides an alternative to a chip based infrastructure.

There was a slight scare in August 2017 when a security threat was discovered that affected 750,000 ID and e-residency cards issued between 2014 and 2017. It was reported that a code library developed by Infineon, which had been in widespread use in security products such as smartcards, had a flaw (later dubbed the ROCA vulnerability) that allowed private keys to be inferred from public keys. Luckily, they had the capabilities in the country to analyse and design a workaround to the system.

In this context, it is important to note that an eID and its technology are the basis of a nation's sovereignty. From the lessons learned in Estonia, we cannot overly rely on one technology in these critical cases, but need to have multiple options between what to choose from. To Estonia, this is very relevant today in EU discussions on the eIDAS2 regulation about the next generation EU digital identity, the EU wallet ecosystem. The solution proposed should not only be under the full control of the user to initiate interactions, the wallets themselves need to be under the full control of the countries that issue them. The dependence on secure hardware components (bearing in mind that no serious smartphone makers are from Europe) is maybe not always advisable, they are hard to replace or cumbersome to modify. Software-based solutions, with the option to quickly modify, upgrade them, is a must and should definitely be stipulated as one technological alternative, especially if it has proved its security and usefulness.

The creation of these two key cybersecurity solutions has enabled Estonia to secure its foundations, create a culture for security and enable it to build quite a sophisticated ecosystem on top of it. Estonians declare their taxes in 30 seconds, do not carry prescriptions, access all of their medical data online, and vote online. In the last elections about 45% of Estonians voted via the web. And that is at the general elections, which no country in the world is actually doing, because of mostly cybersecurity fears. Since 2005 they've been showing the world that the impossible is possible. That subjective fears that often are spread can be overcome with logical research-based argumentation and proof that the technology works as described and not in any other ways. Also, during the 17-year experience that Estonia has been running this system, there have been no security incidents: yes, there have been misinformation campaigns, but no incidents. In the next local elections, they will try out Internet voting system mobile...

Oliver believes that, for all these innovations to succeed, three fundamental things are required: first, understanding the state of the art in technology and research, foresight on how these technologies impact the society or its users and incremental investment in order to keep them alive. As soon as you stop investing in these technologies and the underlying research, the technology becomes vulnerable, it becomes unusable. The complexity of the technology world is increasing, is in constant flux, one needs to invest regularly in order to stay in the game, let alone stay ahead of the game.

So what does the future hold for Cybernetica and Estonia, what are they currently working on?

One aspect that they are keen to understand better is the notion of privacy in the digital world. What are the technologies that enable us to give people more control, more transparency over the usage of their data? Are there any solutions that when deployed, could give data holders competitiveness in the usage of this data in a way that personal data is not revealed, or only revealed when there is a real cause or need for it. Cybernetica has been working on privacy enhancing technologies (PETs) since early 2010, including being part of the last three DARPA privacy programs. Today, we see that the world is getting ready for technologies like secure multiparty computations or zero knowledge proofs - more and more service providers, with even the likes of Meta are coming up with practical needs. The Estonian government has initiated a Privacy Enhancement Technologies program, which is in its infancy today, but probably has great potential for bringing additional guarantees, trust to the owners of the data, but also enables the unlocking of some of the value in confidential data.

Finally, Estonia is not an island, by far. It is a small, micro player in a big pond, it is dependent on everyone in the ecosystem, from browser manufacturers, to hardware producers to operating systems developers. All these stacks have an occasional vulnerability, serious flaw diagnosed that'll have a significant impact on infrastructure like the ROCA vulnerability diagnosed for ID cards in 2017. In order to be safe, there has to be a good operational picture on what is going on in the world, one needs to build coalitions with governments and relevant institutions to get information on possible threats and vulnerabilities as soon as possible. One needs to have the capability to process this information if relevant and have a clear understanding of its impacts. The world is interconnected – one vulnerability might impact in a place where least expected. Some interdependency analysis has been done in Estonia, but there is a lot more to do.

Oliver hoped that his speech gave quite an explicit overview why they believe that investing in cybersecurity is a must. Without these investments one actually cannot guarantee the credibility of a digital ecosystem. The thought of being left out of a cybersecurity competence centre, as was possible when the eventual evaluation results were announced, was disturbing. For Cybernetica, being part of the European ecosystem, is fundamental, especially in today's geopolitical context where they see more and more regionalism.

He was very happy to see that the work done over the last two years on the competence centre pilot program has had real impact. That all four projects have delivered concrete results in their specific domains, like looking at the challenges in, for example, supply chain security assurance or medical data exchange. He was also glad to learn that all four pilot programs are in the process of formulating a unified research roadmap for the Competence Centre Program. Cybernetica already sees that the network has enabled them to strengthen their existing ties but also formulate new ones in the European cybersecurity ecosystem - pursue new projects, create new alliances. It is evident, that when collaborating, they are stronger, better prepared to the challenges that lie ahead.

Finally, he noted that we hope that the European Cybersecurity Competence Network and Centre will leverage the work done in the four pilots and continue the pursuance of their goals, also the facilitation of contacts between different research bodies. At times, looking from Estonia, it is not clear how the new big picture with activities being pursued by national governmental nodes will all fit together into a European wide network. But then again, he was sure that, as with any new initiative, time will sort things out.

4.3 Bart Preneel, Head of Computer Security and Industrial Cryptography (COSIC), KU Leuven

The last session before the evening event on the first day of Momentum! was a keynote speech by Professor Bart Preneel. The talk showed a common understanding with CyberSec4Europe's visions in many important areas.



Figure 16: Bart engaging with the audience

Following the previous talk, Bart agreed on the importance of certification for building secure systems. However, while certification nowadays is mainly focusing on limited components like smart cards, complex systems (e.g., smart phones, computers, etc.) are hardly ever certified, increasing the risk of market failures. As a consequence, current certification schemes need to become more efficient and cheaper, and at the same time significant additional research efforts are required to also certify complex real-world systems. This will also require a paradigm shift from detecting security incidents (e.g., with the help of AI) to building secure systems in the first place.

The task of building secure systems directly leads to the challenge of more secure processing of (outsourced) data. While confidential computing using trusted enclaves such as, for example, Intel SGX or ARM TrustZone, offers one part of the solution, it still requires trust in chip manufacturers or the like. Another important part of the solution is the use of advanced cryptographic primitives such as secure multi-party computation (MPC) or fully homomorphic encryption (FHE), which protects data while it is being processed. These solutions started with an overhead of up to 10^{12} , and now reached sufficient efficiency for certain applications, with an overhead of about 1'000. DARPA is investing money to increase efficiency by an additional factor of up to 100 by hardware support, leading to fully practical solutions there. Unfortunately, while Europe could definitely make a difference here, Bart points out a lack of a clear European strategy and funding in this domain.

Therefore, in order to reach European sovereignty, the European Union may decide to accept, for example, the US as a strategic partner with all the related implications regarding self-sovereignty. If not, Europe needs to build their entire own ecosystem, going beyond the European Chips Act, but also including software, operating systems, network equipment and the like. However, as it might not be feasible to fully rely on EU-only products, a possible way out is the use of end-to-end secure architectures, which could, for example, allow the transfer of sensitive data over potentially insecure network layers (leaving aside the

important challenge of metadata). However, this may lead to tensions with strategies of law enforcement, for example. Therefore, clear policy decisions need to be taken. Furthermore, open systems will play an important role on the way to European sovereignty.

The last major topic of the keynote speech was related to the current research landscape. With many important players such as the ECCC and its national coordination centres (NCCs), ENISA, ECSO, Europol, as well as national governments with major investments in cybersecurity, it is hard to generate a common European vision. This leads to the situation that excellent research is performed within the EU, but final decisions - for example, on the selection of post-quantum cryptography - are taken by NIST. What is thus needed is a politically supported, bottom-up strategy to bring the many different views and approaches together. Finally, Europe needs to continue their large-scale investments in research funding, but should thereby critically question the current approach - while sometimes a novel idea can lead to a market-ready product within a year or two, other research activities require decade(s) to reach maturity, as was the case, for example, with MPC or FHE. This should be better respected by the funding models, where currently most projects have roughly the same duration, such that more flexibility of the funding mechanisms for different research ambitions is required.

5 Evening Panel

The agenda for the evening keynote and panel discussion which followed a short networking break was:

- **Welcome** by **Martin Friedrich Reinhardt** (Head of Unit, Affairs of the Hessian Ministry of the Interior and for Sports, Representation of the State of Hessen to the EU), mentioning the crisis in Europe (including the Russia-Ukraine conflict) and the importance and role of CyberSec4Europe.
- **Keynote:** by **Ievgen Vladimirov** (International Cybersecurity University, Kyiv): entitled “*First-of-a-kind cyber war*” covering information about the history of Russian-Ukrainian conflict in both the physical and cyber spaces and highlighting the importance of cybersecurity in this concept.

Panellists:

- **Tamara Tafra**, Minister Counsellor, Cyber issues, hybrid threats and disinformation, Permanent Representation of Croatia to the European Union
- **Wojciech Wiewiórowski**, European Data Protection Supervisor (EDPS)
- **Katarzyna Prusak-Górniak**, Head of Digital Affairs Unit in Permanent Representation of Poland to the EU, Deputy Chair of the European Cybersecurity Competence Centre Governing Board
- **Francesco Barbato**, Programme Officer, Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission
- **Cláudio Teixeira**, Legal Officer – Digital and Consumer Rights, The European Consumer Organisation (BEUC)

Moderator:

- **Kai Rannenberg**, Goethe University Frankfurt and CyberSec4Europe coordinator



Figure 17: The evening panel discussion

5.1 Cybersecurity in Europe: Past, Present and Future

Martin Friedrich Reinhardt welcomed everyone to the evening panel and introduced a team from the Hessen Code of Audit who were present. He said that we have learned to live with crises and that this is no reason for giving up but that we instead need functioning crisis management. We need to find the right way forward. to protect the critical infrastructure from cyber attacks, but also to build cyber defence. Data protection, law enforcement. Development of resilience in general and cybersecurity in particular. CyberSec4Europe is a strong voice in developing democracy, peace.

Ievgen Vladimirov introduced his keynote speech, 'First-of-a-kind global cyber war' by reminding the audience that life is the most important investment. And the importance comes to people if it is interrupted. War is the disruptor.



Figure 18: Ievgen giving his keynote speech on the line from Kyiv

There are five recognised dimensions or domains of warfare: land, sea, air, space and cyber - the latter added in 2016 by NATO. The fifth is important because it has three interrelated layers of cyberspace. All layers are interconnected. Starlink has helped Ukraine in its cyber defence.



Figure 19: Ievgen's opening slide

The first cyber war was held in Ukraine and it started much earlier in 2014 than the current aggression that started in February 2022. Ukraine was the most targeted country from July 2020 to June 2021. There is a really clear connection between the cyber attacks and what is happening on the ground in Ukraine right now.

Cyber attacks can hit targets much further away than any rocket can reach which we can see with the number of countries that have been targeted. We all have one overriding question: if all of the attacks were military instead, how could we prevent and not make a mistake with a price that might result in a worldwide war?

How to move forward? This is the first real cyber war which has been ongoing already for eight years. We have to research it and draw conclusions for the next generations. We invite you to join on this journey so that we can create the basis for new legislation. We have to understand the difference between military and non-military cyber attacks.

A number of examples:

- 2014 - a cyber attack on the election system at the time of Ukrainian parliamentary elections
- 2014 and 2015 - cyber attacks on the energy grid
- 2021 - the same attack on US critical infrastructure

Any cyber attack on state military and critical infrastructure which causes the failure of a critical service is equivalent to military aggression. If we consider, this then we could be prepared. But we cannot or do not see a cyber attack in the same way as we see attacks on the streets of our cities.

To conclude, we are making a call for collaborative research and European-wide legislation.

Question from the audience: What kind of data do you have?

Answer: All kinds of data which we have been gathering since 2014, collected by government stakeholders, which we are willing to share.

Ievgen's presentation can be viewed on the CyberSec4Europe website³.

Kai introduced the panelists and then started the discussion saying that there were three things that we were not expecting when we were designing CyberSec4Europe or that our momentum would somehow need to cover. Firstly, the Russian attack on Ukraine.

Wojciech: CyberSec4Europe started in 2019 and in the middle of the cyber attacks against Ukraine! Meantime there were several software attacks on thousands of Ukrainian companies. There are several lessons to consider: firstly, war is not just against the military! We were already inside the time of attacks on the Ukraine, and we had examples of the special threats that we have to access (notPetya). This was reused on thousands of companies in Ukraine, including companies that were not expecting this. A bookkeeping company was used as the vessel for distributing the cyber attack.

The second lesson learned as one of the data protection authorities in Europe which tries to raise awareness of data protection is: formal achievements of the countries might not reflect and not be as important as the practical outcomes. Russia also has a strong data protection act. But just because someone has a law, it does not mean that they are in line with the ideals of other countries.

Tamara: We must engage in dialogue with our counterparts from Ukraine: we can help them and also learn from them. Russia is also a part of the UN that has laws for proper conduct in cyberspace and they are not looking at the problem: We can do more together with the Ukrainian side to call upon Russia and bring them to the courts at the international level. We need to talk about this and see how we can do it. The EU has also invested in providing software and hardware to Ukraine - we are not stopping, we are continuing as there are a lot of things that we can do. The issue is that the physical attacks are more severe than the cyber ones. Cyber is not the main focus for that reason but it is important and we are trying to bring it into focus.



Figure 20 Tamara explaining a point

Katarzyna: There is a working group to cooperate with Ukraine in the board of the ECCC, preparing the first meeting of the group to discuss further and look to strengthen the framework for crisis management. By strengthening our resilience, how can we improve the framework, how can we help the people of Ukraine involved in the war. Many have fled and some have entered Poland which united Ukraine's digital wallet

³ <https://cybersec4europe.eu/events/momentum/momentum-report/keynote-speakers/>

with the digital wallet of Poland, so the Ukrainians could have documents. This will hopefully lead to yet more developments with eIDAS.

Francesco: It's good when things work out for a project especially one this large which has had such impact and importance. The ECCC has started its own operations for a cybersecurity strategy of the Union. We have seen the results of cybersecurity aggression. The operational aspect is improving our situational awareness strategies using security operation centres (SOCs) as early as next year. We believe that there is room for improvement, not only to create links but to create links between SOCs across borders. Information sharing is important and also a lesson learned about what we need to do: that is, to share data across borders, and to learn from experiences. Financial resources are being dedicated to improving social awareness and information exchange between Member States and cross border (from the Digital Europe program). We have learnt lessons from the war and about what we could and should do. All this leads to strengthening the competitiveness of Europe leading to strategic autonomy and the creation of space for stakeholders to grow in Europe.

Cláudio: It only shows how relevant cybersecurity is. You might be doing bookkeeping today but everything is interconnected and threats are becoming more dangerous than we could possibly imagine a year ago. NIS2 is the most important legislation: most of the devices that we use all the time are fundamentally unsafe, and vulnerable to attacks. Cyber resilience is of utmost importance. Our infrastructure and cyberspace are vulnerable to attack. This is an opportunity to make and show that we are safe! We should not waste it! The government needs to step up and provide protection. This is changing and needs to be put on the spot.

Kai: The second thing: we need the impact of regulation on the market: which of the long list of regulations plays the biggest role in expectations and hopes?

Katarzyna: We are missing people who will carry out this legislation which is about people, professionals and communities. There is no skilled force, and not enough competences. NIS2 is the most important and we need work on the Cybersecurity Resilience Act (CRA). We should focus on what we already have and be sure to have implemented it.

Francesco: We started to define what we needed for implementation. For me it's the one that creates the competence centre: making the centre operational and financially independent and then scale up the communities across Europe, strengthen European competitiveness and industry in the cybersecurity domain. Implement things with real users. There is an opportunity in European industry and research to needs to meet the requirements of the legislation.

Wojciech: The activity of the people in the Member States is vital. we cannot wait for legislation from the top - this approach is not enough, we have to start from the bottom. Hessen is the place where the data protection law was first taken into effect. They started from the bottom and did not wait for instructions. Skills - the people are around and we do not have to wait but to find them and pass them the skills.

Tamara: Legislation - all are important. Since 2017 and the introduction of the Cybersecurity Act, in five years we have managed to enact three complicated legislative acts and we're working on a fourth one. All of them are interconnected: for example, the CRA gets certification from the Cybersecurity Act. It's important that all the stakeholders are involved. Skills are the most important. We do everything for society and citizens. We need to start thinking about how to bring digital issues closer to our youth. We need to use the opportunity to share the important messages, especially among youth. We need to promote it more! Cybersecurity is not just for the specialists but for all.

Question from Stefan Bumerl: We in Europe are good at identifying the right thing but bad at implementing them. eIDAS has been in place for some time and still there are very few eIDAS-compliant digital signatures out there. NIS2 is upcoming. There is the possibility to get the ball rolling as 160,000 organisations need to be standardised. The wish is to remain onside with our goals and laws. How can we improve the efficiency of implementation?



Figure 21: Stefan asking a question

*Question from **Stelian Brad**:* AI is explainable and trustworthy, but cybersecurity is no way to prove the trustworthiness of a solution. We can accelerate this bottom-up. What do you think?

Wojciech: We do not want to kill industry and their operations. At the time when GDPR was created, the request was not to over-legislate and in the implementation phase we got questions like, "Where are the templates and guidelines?" There is work to do. There is a lot of legislation ongoing but it's not clear why.

Katarzyna: I have huge hopes for eIDAS but you need substantial use cases. People will use wallets only when they see that they are useful. This is the future. We are progressing but maybe not as fast as we would like.

*Question from **Indra Spiecker**:* In the GDPR we have privacy-by-design. Is this something we need in cybersecurity as well so that it is not an add-on at the end. Would this solve things in the end?

Francesco: The CRA is going toward that solution. Anything with digital components needs to be cybersecurity compliant. We can improve.

Tamara: Have the CE marking for cybersecurity as well. So you know that the solution is cyber secure. Also individuals need to have cyber hygiene, but this is going to protect those of us who do not have that good cyber hygiene.

Cláudio: Around half of the devices that are interconnected are not covered by any legislation that requires them to be cyber secure: for example, the GDPR does not give an enforcement framework like the CRA will. This is needed if products are fundamentally unsafe. We need to have these requirements.

*Question from **Luis Antunes, University of Porto**:* There is a lack of trust in the scope of cybersecurity. Otherwise we will not share information. Are we in a position where the trust is in place or do we need face-to-face meetings to build trust?

Wojciech: It is OK to talk about trust at the beginning of a project, but it is sorry to discuss it at the end and after years of cooperation! We will never have the level of trust that we would like. It can be killed by big politics that are not connected in ways that the people and companies want.

Katarzyna: Trust is personal and a work in progress. We have framework networks and these help build trust. There is cooperation within the Council as well

Tamara: It is still ongoing but much better than it used to be.

Francesco: All the activities we do together, we hope will help to build trust.

Luis: If we work as 27 separate countries, we will not win this war.

Kai: How can we deal with that?

Francesco: SOCs and cross-border components support the idea of trust by having common projects for Member States. We are trying to build this and facilitate it at the European level.

Cláudio: Give power to the people. If we have good legislation this should allow us to collaborate. Ensure that we create the means for reporting on these vulnerabilities and also keep manufacturers honest.

As the discussion came to a close, Kai thanked the panellists and gave them each a gift!

6 Key Exploitable Results

In addition to the printed general event agenda for the event, the attendees were given an additional page listing the assets to be presented and an explanatory text to provide the context for the process (*see figure 6*):

"CyberSec4Europe's legacy beyond the end of the project can be seen in the results of the work carried out by all partners over the past four years.

In a series of reports, we highlighted the individual and joint exploitation and innovation plans, involving assets and solutions across the different project domains, ranging from, for example, maritime transport to the Flagship cyber range challenges.

As CyberSec4Europe comprises diverse organisations – from software vendors, commercial businesses, universities, research institutes, SMEs, legal and consultancy firms to not-for-profit organisations – each type of partner has evolved exploitation strategies in line with their own needs and opportunities. And we celebrate each and every one!

At Momentum! we are showcasing six of the key exploitable assets and solutions over the course of the first day. As difficult as it was to narrow down the results to six, our independent jury members – Stelian Brad from Cluj IT Cluster and Stefan Bumerl of CRYPTAS it-Security GmbH – will identify just two to go forward to the European Commission's Horizon Results Platform."

6.1 The six presentations

The six assets and their owner presenters are listed below together with links to the presentations. To watch and listen to the presenters, these can be found in the video recording of the first day of Momentum!⁴

1. OBSIDIAN Sharemind MPC Extensions⁵

Improving the fight against banking fraud ensuring GDPR compliance and banking secrecy
Liina Kamm, Cybernetica AS

(Authors: Liina Kamm, Baldur Kubo, Cybernetica; Mederic Collas, Informatique Banque Populaire)

2. Flagship⁶

A realistic cyber security exercise using a feature rich live cyber range

⁴ <https://www.youtube.com/watch?v=8Fo7PfX2lNA>

⁵ <https://youtu.be/mC0totxhxxk>

⁶ <https://youtu.be/GJV0mZRbg-0>

Jani Pääjärvi, JAMK

3. Replica TEE⁷

Enabling Seamless Replication of SGX Enclaves in the Cloud

Alessandro Sforzin, NEC Laboratories Europe GmbH

(Authors: Claudio Soriente, Ghassan Karame, Wenting Li, Sergey Fedorov, NEC)

4. CaPe⁸

A consent-based personal data suite to manage personal data in compliance with the GDPR

Vincenzo Savarino, Engineering Ingegneria Informatica S.p.A.

5. EBIDS⁹ (An ensemble-based intrusion detection system)

Pushing Intelligence in Threat Sharing Platforms

Giuseppe Manco, Consiglio Nazionale delle Ricerche (CNR)

6. SecCerts: datamining security certification documents¹⁰

An analysis tool for certificates of security products

Petr Švenda, Masaryk University

The speakers were given 15 minutes each, which included time for questions and answers. They were told to imagine that they were presenting to a set of potential investors who already were quite familiar with the description and strengths of their solutions but were looking for that something special that would differentiate them from the others and had a credible opportunity in a competitive marketplace.

The two jurors were able to question the presenters at the end of each presentation and also took the opportunity to discuss with them during the coffee and lunch breaks.

6.2 The jury summing up

At the beginning of the second day of the summit event, Stelian and Stefan together gave a fulsome description of their approach to the task of adjudication. Here is a more or less transcript of their summing up of the process they undertook and their views on innovation that informed their decisions. Their description is also available online¹¹.

Stefan: It started a couple of weeks back when David asked for someone external to look at the efforts of the 43 partners and I asked how much time will be necessary for so many results. I was not part of the project, and they were about many areas of expertise that I had no personal core expertise of, so I expected it to be a bit challenging. We had luck – David and his team did a really good job taking the total number of assets and reducing the shortlist to 13 topics that we should look a little deeper into it.

During the first round we really wanted to create a formal process, to create a number of criteria to use to score the assets.

Based on the answers provided in advance we were able to look at criteria such as the needs and challenges, the business model, the network, the market etc, the project dividend. All of this information was gathered and provided to us in advance of the judging. To go ahead, we originally had three evaluators, and to have a common ranking we had an extensive points system based on sustainability, technology market readiness level, policy priorities they address, reusability, affordability, the power of communities and the green aspect.

⁷ <https://youtu.be/ouG127CaDUU>

⁸ <https://youtu.be/LkocGEaO-6E>

⁹ <https://youtu.be/johb8bUyrlc>

¹⁰ <https://youtu.be/nyMUchrdCbs>

¹¹ <https://youtu.be/XfvKR09QaXA?t=1373>

We narrowed it down to six finalists, and it was really interesting to see in more detail what the projects were really about when presented here – although it didn't make it easier for us!

The goal however was not to stick to simply numbers and points, and we had a lot of discussion about all of the original points we had scored. We tried to look at our role as potential investors.

Stelian: Firstly, I would like to congratulate all the finalists because in our view you did a great job. We have seen the implications of all the teams and from this perspective all are winners. Difficult to compare apples with pears for as you have seen each project was focussed on a different area. We looked at each one's innovation readiness level (which is different from market readiness): every detail of the capability of transferring to be adopted by the market is important. From this perspective I'd like to introduce these projections of innovation for you and I hope you will all understand I make an assessment of your work where you have strengths and where you might have to improve. Maybe from this point of view, you will learn how to reposition yourselves.

About technology readiness it is something that has been introduced, in the pre-selection phase. What was very important to the jury was to differentiate. Both Stefan and I had experience in the market of related products and it is a highly competitive space.

The capacity to differentiate by strategy, by value proposition, by IP (intellectual property) readiness level, from similar technologies, or substitute technologies in the market – we have related experience in these highly competitive markets. The capacity to provide blue ocean space to create radical innovation or disruptive innovation is important. We look where there were gaps in the market that need to be filled with something because, if an ecosystem is not functional because it has a gap, that creates a problem for all of us. This was an important criterion.

Also we had to look at other criteria such as the IP readiness level – in some cases the patents. Patents are OK but they have a value associated with certain business models. Otherwise, they have no value. Here, I have to make a comment about the weakness of the European landscape. We are encouraged by the Commission to fund these projects and push them to publish their results because once published they become public good for all of us, not just Europeans, but the world. However, I feel aligned with Professor Bart Preneel's comments yesterday that sometimes in our European innovation landscape is difficult – the businesses which are driven by radical, disruptive technologies we have to take care of how we tackle intellectual property e.g., the example of DARPA.

In terms of market readiness, some of the projects were easier to be introduced, some were needing more work to educate the market for adoption. Sometimes we have to go deeper to understand the behaviours of the market to adopt – and sometimes we have to care for the end users. What will be done with the results further? We need the projects to highlight this and explain what they want to do further. We need to see commitment to move forward rather than just an intellectual exercise to demonstrate professionalism or creativity, and, when seeking capital for finance, we expect to see some more sense of this from the project presenters. Something about the readiness of the company, something about the scalability. We tried to interact with the presenters to find out more information. Also, the capacity to deploy in different locations – that's an important issue. These factors shaped our final decisions.

Some projects are ready now to be in the market, and some need more attention and maybe more encouragement, but they have a huge potential in the cybersecurity landscape. These criteria together shaped the decisions on the winners.

Stefan: We had partners from industry and some from academia and we wondered if this should also shape our decision because of the different backgrounds they originated from. My expectation was there should be a gap between them, but we decided to give two awards which meant we could get round this problem. We decided to give an award to one from each category.

Announcement!

Stefan: The first winner is a clever idea, a new idea – a new idea that makes you think, why isn't that standard out there, because in supply chains, in terms of software sub-components, you need to have a way to address the challenge. You know you have on the one hand commercial supply chains contributing to any product however the reality is that you have a lot of sub-contractors and you don't know how many components are embedded in the product which can affect them. That kind of process you need to map these CVD (coordinated vulnerability disclosure) reports on a daily basis and how they are affecting us – if you are not a vendor yourself and you are working with many vendors you cannot understand how faults might be affecting you: it may not be good enough to rely on their reports. SecCerts had that idea and created the mapping - whenever you identify something broken you can see what else needs to be changed. This idea has a lot of potential and I would apply that kind of methodology to the reports coming out of certification, if you are using open source you are forced to mention in the documentation to see what is claimed to be embedded. To have a quick open source library to see what is embedded. So the first winner is SecCerts!

Stelian: I would also like to add something – apart from the name which was interesting, but ... they open a new space of consolidating our cyber resilience in Europe. Because if we move a little bit forward to think about innovation, it is not always the most important thing but consolidation of the business environment is also important. We can align these with the forthcoming rights enshrined in the Cyber Resilience Act and align these with strong customer rights.

The trophy is awarded!

Stelian: It's my turn to introduce the second winner. Also because the asset is a niche product: that is, it addresses a niche area which is very important and also the passion you transmit to the public about the product is very important: the courage to demonstrate uniqueness – something that is difficult to replicate by anyone to consolidate European cybersecurity.

To contribute to the resilience of the cybersecurity of Europe was one way the product fulfils this requirement.

Yesterday we interrogated this winner a lot because we realised that they are capable of creating an automatic system that will strengthen the capacity of firewalls and other devices in order to identify any suspicious behaviours. You need to work more on the promotion of this product.

Stefan: We advise that you should look at promoting this product to vendors within the OT field because you have quite different systems in the OT field your technology could be adaptive enough to cope there.

The second trophy is awarded to EBIDS!

Antonio Skarmeta, the session moderator, thanked the jury, observing how fundamental it is to have external views on the work we do and complimented them on having done a very good job!



Figure 22: Stelian describing the jurors' approach to innovation

Figure 23: Stefan announcing one of the winners



6.3 The winners



Figure 24: Stelian and Stefan with Vashek Matyas, receiving the trophy on behalf of SecCerts



Figure 25: Stelian and Stefan with Giuseppe Manco, with his trophy for EBIDS

For more on the background to CyberSec4Europe's work on exploitable results, see deliverable report D9.27 Exploitation Strategy 3.

7 Application Demonstrator: Supply Chain Security

Martin Wimmer lines out that the topic of supply chain is very broad. With this presentation he aims to show how to support and control the stakeholders of supply chains. Martin Wimmer lines out that this demonstration is to be understood as a teaser. The demonstration was built with synergies between WP3, 4 and 5. The results we have are good but in WP9 we come up with concrete recommendations. While things are produced, designed, and developed monitoring is required to identify issues. The first use case is about retail business and the second is about a custom way for the end customer. A digital version of the supply chain enables monitoring and ensuring that suppliers follow the rules. Relationships of manufacturers, suppliers and sub-suppliers are taken into account to keep the quality high. To overcome the issue of revealing secret information for the sub-supplier to, for example, the manufacturer, the blockchain technology was chosen. In their architecture they chose a three-tier representation. The user interface was designed for the engine with the aim to verify, achieve and validate that the technology works as expected. Furthermore, Martin outlined the interaction between the deliverables and provides selected examples such as feedback taken to the roadmap and is coming up with concrete recommendations.

A final question to be answered is whether blockchain is the right choice for supply chain. He starts by analyzing the technological environment within the recent years using the Gartner hype cycle and presents influencing technologies, e.g. smart contracts, consensus mechanisms, decentralized application, and others. He concludes that we can use blockchain to enforce business compliance, to ensure non-repudiation and ease dispute resolution but the setup and operation of decentralized systems imply additional costs and efforts. He also lines out the demand for future research and development to ease the use of blockchain technology.

Question from the audience: What are the pain points of the players in the supply chain. How difficult is traceability?

Martin: We did not choose a use case for blockchain, we did it the other way round. The aim was to digitise the supply chain. Building up trust without a trusted party was one of the key goals.

Question from the audience: The USA is stopping its activities in the Far East? What does that mean for the European Union?

Martin: The EC has split with markets. We want to be in a position to trade with all of them.

Question from the audience: Who is liable if something fails in, for example, a multi-country supply chain?

Martin: We do not have all the answers yet. Basically, you cannot build up a system without the stakeholders. However, there is a traceability of documents in cases of conflict that works in the use case provided.

8 Seizing The Momentum!

The final panel session featured all of the work package leaders who were scattered around the hall and responded in turn to prompts from Kai Rannenberg who coordinated the session.

[WP2] **Natalia** gave an overview of what has happened during these times, and, despite the challenges, we have persevered and built a community.

[WP3] **Antonio** mentioned the impressive integration that has been done to produce the results. Research, collaboration and integration

[WP4] **Evangelos** highlighted the collaboration inter- and intra-pilots which is reflected in the deliverables. The Blue Book is something to be remembered in the future.

[WP5] **Alessandro** echoed Antonio and Evangelos on collaborations. Finding the common theme among the diversity of the deliverables and tasks was a challenge that was successfully managed.

[WP6] **Jarno** mentioned having to go through all the global frameworks (more than 15 different areas) and 500 subtopics, and putting into a work group into 55 skills. You can see it in the deliverable D6.6.

[WP7] **Vashek** was still thrilled that SecCerts was one of the successful results of the project! He thanked the team for the Flagship support, certificate supports, Cybernetica, interaction with WP6 and the appreciation for the CyberSec sandbox.

[WP8] **Liina** was grateful for the networking and the collaboration. She felt that recommendations were the achievement to be mentioned, as well as the standardisations.

[WP9] **David** picked up on Kai's observation that 43 partners can be easier to manage than ten and went on to remark that this event has shown the achievement in terms of how well everyone gets on with each other, working closely together across all work packages and that is a credit to Kai's leadership.

[WP10] **Mark** stated that it was the most interesting challenging to take and continue - a cybersecurity flagship. We were the only pilot who put all the pilots and ECSO together into concertation events. Our legacy is putting all the pieces together within the concept of Trust in Digital Life. He believed that we were the primary pilot project and thanked everyone and Kai, the coordinator.

Kai then asked each of the work package leaders, this time in reverse order to address what were the important things to do in the future:

Mark: The community exists and will continue. We need to push for funding to get more aspects from it. We should consider the tenders to look after. Funding should be continued at both national and European levels. and we need to make sure SMEs are one of the priorities.

David: We have built a community and we should not let it go. We can make our very best efforts. As Europeans we are missing some points that as a community we can push policy makers to get the story continued. This is not the beginning of the end, but just the end of the beginning. We can help to protect the future of Europe.

Liina: We need to make practical deployment of the research into the technology. We can help others also with the standardization (by the standards matrix).

Vashek: The future is bright! The future is open! We have started the discussions to go forward with our current developed tools (including SecCerts).

Jarno: Also had a dream - working for an NCC and being asked to carry out some tasks which highlighted the education challenge to get people into the right jobs and professions.

Alessandro: The software we produced should be used, deployed and utilised in the future.

Evangelos: We will continue the roadmapping approach. We have created the research roadmap and need to continue.

Antonio: The review is coming and we need to collect the outcomes. The future is blue! Our countries are providing some funds that we need to continue and demonstrate our existence!

Natalia: Don't forget the community. CHECK! Think of it and be inspired.

Afonso asked if he could make an announcement. We have had a big, ambitious and creative project, we have friends from the NCCs and we have expertise in cybersecurity. Afonso said that he convinced his organisation, CNRS, to make a limited amount of money available to keep the community connected through a new project, EU-CHECK, which has 11 CyberSec4Europe partners. We have money on the table and legitimacy, so we could have some spin-offs from CyberSec4Europe as we did before.

David then sang a paean to CyberSec4Europe based on the tune of a well-known bolero song from Mexico.

Finally, **Kai** presented gifts of thanks to **Charlotte Schrauben**, **Christine Jamieson** and **Romy Goodman** for their hard work in making Momentum! a highly successful and memorable event.

9 Summary

The end of the Momentum! summit event marked the pinnacle of the achievements of the CyberSec4Europe pilot project. So much was achieved over these four years which these two days reflected as far as was possible given the time available. It proved to be a satisfying and emotional end to a collaboration that involved so many partners and diverse activities that ultimately coalesced and as a whole was greater than the sum of its parts.

Despite the finality - at least of the funding - the title of the event, Momentum!, was chosen as it owed more to looking forward with hope and energy than simply looking back reflectively - and there is enough to suggest that the community that has been created will in various shapes and forms continue to engage in the furtherance of cybersecurity research for several years to come.

Forward with Momentum!

Annex A: Momentum! Press Release

21/12/2022, 17:55

CyberSec4Europe Hosts Momentum! a Two Day Cybersecurity Summit Event



CyberSec4Europe Hosts Momentum! a Two Day Cybersecurity Summit Event



BRUSSELS, BELGIUM, December 1, 2022 /EINPresswire.com/ -- CyberSec4Europe², a Horizon 2020 pilot project, are hosting an unmissable two-day event, **Momentum!**¹, on 1 and 2 December at the Representation of the State of Hessen in central Brussels and also streaming live. With the creation of the European Cybersecurity Competence Centre in Bucharest and the establishment of National Competence Centres, cybersecurity experts from the project will present their vision on how the European cybersecurity community will continue to collaborate over the coming years.

Our keynote speakers will share their insights and future expectations from the perspectives of technology, industry, politics and cyber war and its social impact. They include:

- Mario Campolargo, Secretary of State for Digitalisation and Administrative Modernisation, Government of Portugal
- Oliver Väärtnöu, CEO, Cybernetica AS
- Professor Bart Preneel, Head of Computer Security and Industrial Cryptography (COSIC), KU Leuven

The conference includes an evening panel discussion and social event, featuring a keynote and special guest speakers sharing their thoughts and discussing, 'Cybersecurity in Europe: Past, Present and Future.'

From the frontline of cybersecurity challenges, Ievgen Vladimirov, a founder and honorary member of the International Cybersecurity University, will give a keynote address on a live link from Kyiv.

Other guest speakers and panellists include:

- Tamara Tafra, Minister Counsellor, Cyber Issues, hybrid threats and disinformation, Permanent Representation of Croatia to the European Union
- Wojciech Wiewiórowski, European Data Protection Supervisor (EDPS)
- Katarzyna Prusak-Górnica, Head of Digital Affairs Unit in Permanent Representation of Poland to the EU, Deputy Chair of the European Cybersecurity Competence Centre Governing Board
- Francesco Barbato, Programme Manager, Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission
- Cláudio Teixeira, Legal Officer – Digital and Consumer Rights, The European Consumer Organisation (BEUC)

“

At Momentum! CyberSec4Europe's 43 partner consortium celebrate the breadth and creativity of European cybersecurity that will positively protect Europe's citizens and society over the coming years.” — Professor Dr. Kai Rannenberg

Another highlight of the event will be the demonstration of six shortlisted project 'key exploitable and innovative results' which an independent jury will then review. Project leaders will showcase their achievements on governance to standardisation, from blueprint research to skills training and also share their visions for the future in each of these areas.

<https://www.einpresswire.com/article-print/604142945/cybersec4europe-hosts-momentum-a-two-day-cybersecurity-summit-event>

1/2

21/12/2022, 17:55

CyberSec4Europe Hosts Momentum! a Two Day Cybersecurity Summit Event

All in all, this will be a memorable opportunity to discover what Europe has learnt and hear expert visions for the way forward for the European cybersecurity community.

The event webpage is <https://cybersec4europe.eu/events/momentum/>.

Lead co-ordinator, Professor Dr. Kai Rannenberg, Goethe University Frankfurt, says: "CyberSec4Europe formed as a strong consortium with partners in 20 EU Member States and two Associated Countries, who aimed to not only strengthen the EU position in cybersecurity but also to enhance the concept of European cybersecurity by keeping it connected with European values like freedom and respect for the individual as well as protection for the most vulnerable, when they most need it. In a nutshell the purpose of Momentum! is to celebrate the breadth and creativity of the many approaches to advancing the European cybersecurity agenda and to demonstrate how Europe will positively protect its citizens and society over the coming years."

About CyberSec4Europe

After four years, funding for CyberSec4Europe and its 43 consortium and many associate partners will end in December 2022, having collaborated creatively and effectively across many different cybersecurity domains.

The CyberSec4Europe pilot project is a research-based consortium with 43 participants from 20 EU Member States and two Associated Countries. CyberSec4Europe was funded to pilot the establishment of a European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, legislation for which came into force on 20 May 2021.

CyberSec4Europe partners address 14 key cybersecurity domains, 11 technology/ application elements and nine crucial vertical sectors. With participation in over 100 cybersecurity projects amongst them, CyberSec4Europe partners had the considerable experience to address a comprehensive set of issues across the cybersecurity domain. The project demonstration cases addressed cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, health and medicine and maritime transport. In addition to the demonstration of a proposed governance structure and operation of the network, CyberSec4Europe developed a strategic roadmap and recommendations to help drive future cybersecurity-related funding programme calls, including those in Horizon Europe and Digital Europe.

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929

David Goodman

Trust in Digital Life

david@trustindigitalife.eu

Visit us on social media:

[Twitter](#)

[LinkedIn](#)

¹ <https://cybersec4europe.eu/events/momentum/>

² <https://cybersec4europe.eu>


This press release can be viewed online at: <https://www.einpresswire.com/article/604142945/>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.


© 1995-2022 Newsmatics Inc. All Right Reserved.

Figure 26: The EIN Presswire release

Annex B: ECCC Newsletter



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE



NEWSROOM

[European Cybersecurity Competence Centre](#)
[Topics](#)
[Archives](#)

[OVERVIEW](#) > [NEWS](#)

Momentum!

CyberSec4Europe is delighted to announce the agenda for its unmissable two-day event, Momentum!, on 1 and 2 December at the Representation of the State of Hessen in central Brussels.

date: 16/11/2022

Our keynote speakers will share their visions and expectations for the coming years from the perspectives of technology, industry, politics and cyber war and its social impact. They include:

- **Mário Campolongo**, Secretary of State for Digitalisation and Administrative Modernisation, Government of Portugal
- **Oliver Völlmrich**, CEO, Cybernetica AS
- **Professor Bart Preneel**, Head of Computer Security and Industrial Cryptography (COSIC), KU Leuven

The conference also includes an evening social event, featuring a keynote and special guest speakers sharing their thoughts and discussing, 'Cybersecurity in Europe: Past, Present and Future.'

We are honoured to have the following keynote and guest speakers:

Keynote:

- **Ievgen Vladimirov**, General Director, International Cybersecurity University, Kyiv

Guest speakers:

- **Tamara Tafra**, Minister Counsellor, Cyber issues, hybrid threats and disinformation, Permanent Representation of Croatia to the European Union
- **Wojciech Wiewiórowski**, European Data Protection Supervisor (EDPS)
- **Katarzyna Prusak – Górnalek**, Head of Digital Affairs Unit in Permanent Representation of Poland to the EU, Deputy Chair of the European Cybersecurity Competence Centre Governing Board
- **Miguel González-Sánchez**, Head of Cybersecurity Technology and Capacity Building, DG CONNECT, European Commission
- **Claudia Teloeira**, Legal Officer – Digital and Consumer Rights, The European Consumer Organisation (BEUC)

Another highlight of the event will be the demonstration of six shortlisted project 'key exploitable and innovative results' which an independent jury will then review. In addition, our work leaders will showcase their achievements on governance to standardisation, from blueprint research to skills training and also share their visions for the future in each of these areas.

All in all, this will be a memorable opportunity to discover what we have learnt and understand our vision for the way forward for the European cybersecurity community.

The event webpage is <https://cybersec4europe.eu/events/momentum/>.

[Register \(for free\) now!](#)

Figure 27: The ECCC news article on Momentum!